

14
15
16
17
18
19
20
21
22
23
24
25

$$C_k \equiv M_k^{e_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

\vdots

$$M_k \equiv M \pmod{p_k},$$

$$e_1 \equiv e \pmod{(p_1 - 1)},$$

$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

\vdots

$$e_k \equiv e \pmod{(p_k - 1)},$$

where e is a number relatively prime to $(p_1 - 1)$, $(p_2 - 1)$, ..., and $(p_k - 1)$,

solving said subtasks to determine results $C_1, C_2 \dots C_k$,

combining said results of said subtasks in accordance with a fast recursive combining process to produce said ciphertext word signal C whereby,

$$Y_i \equiv Y_{i-1} + [(C_i - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n}$$

$$2 \leq i \leq k, \text{ and}$$

$$C = Y_k, Y_1 = C_1, \text{ and } w_i = \prod_{j < i} p_j$$

whereby processing of a minimal amount of computer instructions is required for said step of encoding.

15. (Twice Amended) A method for establishing cryptographic communications that are backwards compatible with preexisting public key infrastructures, comprising the steps of:
decoding a ciphertext word C to a message word M , wherein M corresponds to a number representative of a message and wherein,

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater than 2[,] and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number representative of an

8 encoded form of message word M that is encoded by transforming said message word M to said
9 ciphertext word C whereby,

$$10 \quad C \equiv M^e \pmod{n},$$

11 and wherein e is a number relatively prime to (p_1-1) , (p_2-1) , ..., and (p_k-1) ,

12 said decoding step being performed using a decryption exponent d that is defined by

$$13 \quad d \equiv e^{-1} \pmod{(p_1-1)(p_2-1) \dots (p_k-1)},$$

14 said decoding step including the steps of,

15 (i) defining a plurality of k sub-tasks in accordance with

$$16 \quad M_1 \equiv C_1^{d_1} \pmod{p_1},$$

$$17 \quad M_2 \equiv C_2^{d_2} \pmod{p_2},$$

18 \vdots

$$19 \quad M_k \equiv C_k^{d_k} \pmod{p_k},$$

20
21 where

$$22 \quad C_1 \equiv C \pmod{p_1},$$

$$23 \quad C_2 \equiv C \pmod{p_2},$$

24 \vdots

$$25 \quad C_k \equiv C \pmod{p_k},$$

$$26 \quad d_1 \equiv d \pmod{(p_1 - 1)},$$

$$27 \quad d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

28 \vdots

$$29 \quad d_k \equiv d \pmod{(p_k - 1)},$$

30
31 (ii) solving said sub-tasks to determine results M_1, M_2, \dots, M_k , and

32 (iii) combining said results of said subtasks in accordance with a fast recursive combining

33 process to produce said message word M in accordance with,

$$34 \quad Y_i \equiv Y_{i-1} + [(M_i - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n}$$

35 where $2 \leq i \leq k$, and

36 $M = Y_k, Y_1 = M_1, \text{ and } w_i = \prod_{j < i} p_j$

37 whereby processing of a minimal amount of computer instructions is required for said
38 step of decoding.

1 16. (Twice Amended) A cyptographic communications system for establishing communications
2 that are backwards compatible with preexisting public key infrastructures, comprising:

3 a communication medium;

4 [an] encoding means coupled to said communication medium and adapted for
5 transforming a transmit message word M to a ciphertext word C and for transmitting said
6 ciphertext word C on said medium, where M corresponds to a number representative of a
7 message, and

8 $0 \leq M \leq n-1$ where n is a composite number of the form

9 $n = p_1 \cdot p_2 \cdot \dots \cdot p_k,$

10 where k is an integer greater than 2 and p_1, p_2, \dots, p_k are distinct random prime numbers,
11 and where C corresponds to a number representative of an enciphered form of said message, and
12 corresponds to

13 $C \equiv M^e \pmod{n},$

14 where e is a number relatively prime to $(p_1-1), (p_2-1), \dots,$ and (p_k-1) ; and

15 [a] decoding means coupled to said communication medium and adapted for receiving C
16 via said medium and for transforming C to a receive message word M' where M' corresponds to
17 a number representative of a deciphered form of C, said decoding means being operative to
18 perform a decryption process using a decryption exponent d that is defined by

19 $d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$

20 said decryption process including the steps of

21 (i) defining a plurality of k sub-tasks in accordance with,

22 $C_1 \equiv C \pmod{p_1},$

23 $C_2 \equiv C \pmod{p_2},$

24 \vdots

25 $C_k \equiv C \pmod{p_k},$

26 where,

27 $d_1 \equiv d \pmod{(p_1 - 1)},$

28 $d_2 \equiv d \pmod{(p_2 - 1)},$

29 \vdots

30 $d_k \equiv d \pmod{(p_k - 1)},$

31

32 $M_1' \equiv C_1^{d_1} \pmod{p_1},$

33 $M_2' \equiv C_2^{d_2} \pmod{p_2}, \text{ and}$

34 \vdots

35 $M_k' \equiv C_k^{d_k} \pmod{p_k},$

36 (ii) solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

37 (iii) combining said results of said subtasks by a fast recursive combining process to
38 produce said receive message word M' in accordance with

39
$$Y_i \equiv Y_{i-1} + [(M_i' - Y_{i-1}) (w_i^{-1} \pmod{p_i}) \pmod{p_i}] \cdot w_i \pmod{n}$$

40 where $2 \leq i \leq k$ and

41 $M' = Y_k, Y_1 = M_1, \text{ and } w_i = \prod_{j < i} p_j,$

42 [whereby] wherein $M' = M.$

1 17. (Once Amended) A method for establishing cryptographic communications that are
2 backwards compatible with preexisting public key infrastructures, comprising the steps of:

3 encoding a plaintext message word M to a ciphertext word C , wherein M corresponds to
4 a number representative of a message and wherein

5
$$0 \leq M \leq n-1,$$

6 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer
7 greater than 2[,] and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number
8 representative of an encoded form of message word M , and wherein said encoding step
9 comprises transforming said message word M to said ciphertext word C , whereby

10
$$C \equiv M^e \pmod{n},$$

11 and wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots, \text{ and } (p_k-1);$ and

12 decoding said ciphertext word C to a receive message word M', said decoding step being
13 performed using a decryption exponent d that is defined by

$$14 \quad d \equiv e^{-1} \bmod ((p_1-1)(p_2-1) \dots (p_k-1)),$$

15 said decoding step including the further steps of,

16 defining a plurality of k sub-tasks in accordance with

$$17 \quad M_1' \equiv C_1^{d_1} \pmod{p_1},$$

$$18 \quad M_2' \equiv C_2^{d_2} \pmod{p_2},$$

19 \vdots

$$20 \quad M_k' \equiv C_k^{d_k} \pmod{p_k},$$

21 wherein

$$22 \quad C_1 \equiv C \pmod{p_1},$$

$$23 \quad C_2 \equiv C \pmod{p_2},$$

24 \vdots

$$25 \quad C_k \equiv C \pmod{p_k},$$

$$26 \quad d_1 \equiv d \pmod{(p_1 - 1)},$$

$$27 \quad d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

28 \vdots

$$29 \quad d_k \equiv d \pmod{(p_k - 1)},$$

30 solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

31 combining said results of said sub-tasks to produce said receive message word

32 M', [whereby] wherein $M' = M$.

1 22. (Once Amended) A cyptographic communications system for establishing communications
2 that are backwards compatible with preexisting public key infrastructures, comprising:

3 a communication medium;

4 [an] encoding means coupled to said communication medium and adapted for
5 transforming a transmit message word M to a ciphertext word C and for transmitting said

6 ciphertext word C on said medium, wherein M corresponds to a number representative of a
7 message, and

8 $0 \leq M \leq n-1$, wherein n is a composite number of the form,

9
$$n = p_1 \cdot p_2 \cdot \dots \cdot p_k$$

10 wherein k is an integer greater than 2[,] and p_1, p_2, \dots, p_k are distinct random prime
11 numbers, and wherein said ciphertext word C corresponds to a number representative of an
12 enciphered form of said message and corresponds to

13
$$C \equiv M^e \pmod{n},$$

14 wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots$, and (p_k-1) ; and

15 [a] decoding means communicatively coupled with said communication medium for
16 receiving said ciphertext word C via said medium, said decoding means being operative to
17 perform a decryption process for transforming said ciphertext word C to a receive message word
18 M', wherein M' corresponds to a number representative of a deciphered form of C, said
19 decryption process using a decryption exponent d that is defined by

20
$$d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

21 said decryption process including the steps of

22 defining a plurality of k sub-tasks in accordance with

23
$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

24
$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

25
$$\vdots$$

26
$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

27 wherein

28
$$C_1 \equiv C \pmod{p_1},$$

29
$$C_2 \equiv C \pmod{p_2},$$

30
$$\vdots$$

31
$$C_k \equiv C \pmod{p_k},$$

32
$$d_1 \equiv d \pmod{(p_1 - 1)},$$

33
$$d_2 \equiv d \pmod{(p_2 - 1)},$$

35

36

$$d_k \equiv d \pmod{(p_k - 1)},$$

37

solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

38

combining said results of said sub-tasks to produce said receive message word M'

39

whereby $M' = M$.

1 27. (Once Amended) A method for establishing cryptographic communications that are

2 backwards compatible with preexisting public/key infrastructures, comprising the step of:

3 encoding a plaintext message word M to a ciphertext word C , wherein M corresponds to

4 a number representative of a message, and

$$5 \quad 0 \leq M \leq n-1,$$

6 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, wherein k is an integer

7 greater than 2[,] and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein the ciphertext

8 word C is a number representative of an encoded form of message word M , wherein said step of

9 encoding includes the steps of

10 defining a plurality of k sub-tasks in accordance with

$$11 \quad C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$12 \quad C_2 \equiv M_2^{e_2} \pmod{p_2},$$

13 \vdots

$$14 \quad C_k \equiv M_k^{e_k} \pmod{p_k},$$

15 where

$$16 \quad M_1 \equiv M \pmod{p_1},$$

$$17 \quad M_2 \equiv M \pmod{p_2},$$

18 \vdots

$$19 \quad M_k \equiv M \pmod{p_k},$$

20

$$21 \quad e_1 \equiv e \pmod{(p_1 - 1)},$$

$$22 \quad e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

23

24

$$e_k \equiv e \pmod{(p_k - 1)},$$

25

wherein e is a number relatively prime to (p_1-1) , (p_2-1) , ..., and (p_k-1) ,

26

solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and

27

combining said results of said sub-tasks to produce said ciphertext word C .

1 32. (Once Amended) A cyptographic communications system for establishing
2 communications that are backwards compatible with preexisting public key infrastructures,
3 comprising:

4 a communication medium;

5 [an] encoding means coupled to said communication medium and operative to transform
6 a transmit message word M to a ciphertext word C , and to transmit said ciphertext word C on
7 said medium, wherein M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

8
9 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$ wherein k is an integer
10 greater than 2[,] and p_1, p_2, \dots, p_k , are distinct random prime numbers, and wherein the ciphertext
11 word C is a number representative of an encoded form of message word M , said encoding means
12 being operative to transform said transmit message word M to said ciphertext word C by
13 performing an encoding process comprising the steps of

14 defining a plurality of k sub-tasks in accordance with

$$15 \quad C_1 \equiv M_1^{e_1} \pmod{p_1},$$

$$16 \quad C_2 \equiv M_2^{e_2} \pmod{p_2},$$

17

$$\vdots$$

$$18 \quad C_k \equiv M_k^{e_k} \pmod{p_k},$$

19

where

$$20 \quad M_1 \equiv M \pmod{p_1},$$

$$21 \quad M_2 \equiv M \pmod{p_2},$$

22

$$\vdots$$

23 $M_k \equiv M \pmod{p_k},$

24

25 $e_1 \equiv e \pmod{(p_1 - 1)},$

26 $e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$

27 \vdots

28 $e_k \equiv e \pmod{(p_k - 1)},$

29 wherein e is a number relatively prime to (p_1-1) , (p_2-1) , ..., and (p_k-1) ,

30 solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and

31 combining said results of said sub-tasks to produce said ciphertext word C .

1 37. (Once Amended) A method for establishing cryptographic communications that are
2 backwards compatible with preexisting public key infrastructures, comprising the steps of:

3 decoding a ciphertext word C to a message word M , wherein M corresponds to a number
4 representative of a message and wherein

5 $0 \leq M \leq n-1$

6 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater
7 than 2[,] and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number representative of an
8 encoded form of message word M that is encoded by transforming said message word M to said
9 ciphertext word C whereby

10 $C \equiv M^e \pmod{n},$

11 and wherein e is a number relatively prime to (p_1-1) , (p_2-1) , ..., and (p_k-1) ;

12 said decoding step being performed using a decryption exponent d that is defined by

13 $d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$

14 wherein said step of decoding includes the steps of

15 defining a plurality of k sub-tasks in accordance with

16 $M_1 \equiv C_1^{d_1} \pmod{p_1},$

17 $M_2 \equiv C_2^{d_2} \pmod{p_2},$

18 \vdots

19 $M_k \equiv C_k^{d_k} \pmod{p_k},$

wherein

$$C_1 \equiv C \pmod{p_1},$$

$$C_2 \equiv C \pmod{p_2},$$

\vdots

$$C_k \equiv C \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

\vdots

$$d_k \equiv d \pmod{(p_k - 1)},$$

solving said sub-tasks to determine results M_1, M_2, \dots, M_k , and

combining said results of said sub-tasks to produce said message word M .

42. (Once Amended) A cryptographic communications system for establishing communications that are backwards compatible with preexisting public key infrastructures, comprising:

a communication medium;

[a decoding means] communicatively coupled with said communication medium for receiving a ciphertext word C via said medium, and being operative to transform said ciphertext word C to a receive message word M' , wherein a message M corresponds to a number representative of a message and wherein,

$$0 \leq M \leq n-1$$

wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer greater than 2[,], and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein said ciphertext word C is a number representative of an encoded form of said message word M that is encoded by transforming M to said ciphertext word C whereby,

$$C \equiv M^e \pmod{n},$$

and wherein e is a number relatively prime to $(p_1-1), (p_2-1), \dots$, and (p_k-1) ;

said decoding means being operative to perform a decryption process using a decryption exponent d that is defined by

$$d \equiv e^{-1} \pmod{((p_1-1)(p_2-1) \dots (p_k-1))},$$

18 said decryption process including the steps of

19 defining a plurality of k sub-tasks in accordance with,

20
$$M_1' \equiv C_1^{d_1} \pmod{p_1},$$

21
$$M_2' \equiv C_2^{d_2} \pmod{p_2},$$

22
$$\vdots$$

23
$$M_k' \equiv C_k^{d_k} \pmod{p_k},$$

24 wherein,

25
$$C_1 \equiv C \pmod{p_1},$$

26
$$C_2 \equiv C \pmod{p_2},$$

27
$$\vdots$$

28
$$C_k \equiv C \pmod{p_k},$$

30
$$d_1 \equiv d \pmod{(p_1 - 1)},$$

31
$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

32
$$\vdots$$

33
$$d_k \equiv d \pmod{(p_k - 1)},$$

34 solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and

35 combining said results of said sub-tasks to produce said receive message word

36 M' , whereby $M'=M$.

1 47. (Once Amended) A method for generating a digital signature comprising the step of:

2 signing a plaintext message word M to create a signed ciphertext word C , wherein M

3 corresponds to a number representative of a message, and

4
$$0 \leq M \leq n-1,$$

5 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, wherein k is an integer

6 greater than 2[,] and p_1, p_2, \dots, p_k are distinct random prime numbers, and wherein the signed

7 ciphertext word C is a number representative of a signed form of message word M , wherein

8
$$C \equiv M^d \pmod{n}, \text{ and}$$

9 wherein said step of signing includes the steps of

defining a plurality of k sub-tasks in accordance with

$$C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$C_2 \equiv M_2^{d_2} \pmod{p_2},$$

$$\vdots$$

$$C_k \equiv M_k^{d_k} \pmod{p_k},$$

where

$$M_1 \equiv M \pmod{p_1},$$

$$M_2 \equiv M \pmod{p_2},$$

$$\vdots$$

$$M_k \equiv M \pmod{p_k},$$

$$d_1 \equiv d \pmod{(p_1 - 1)},$$

$$d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

$$\vdots$$

$$d_k \equiv d \pmod{(p_k - 1)},$$

wherein d is defined by

$$d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$$

e is a number relatively prime to $(p_1 - 1)$, $(p_2 - 1)$, ..., and $(p_k - 1)$,

solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and

combining said results of said sub-tasks to produce said ciphertext word C .

52. (Once Amended) A digital signature generation system comprising:

a communication medium;

[a] digital signature generating means coupled to said communication medium and operative to transform a transmit message word M to a signed ciphertext word C , and to transmit said signed ciphertext word C on said medium, wherein M corresponds to a number representative of a message, and

$$0 \leq M \leq n-1,$$

8 n being a composite number formed from the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$ wherein k is an integer
9 greater than 2[,] and p_1, p_2, \dots, p_k , are distinct random prime numbers, and wherein the signed
10 ciphertext word C is a number representative of a signed form of said message word M, wherein

$$11 \quad C \equiv M^d \pmod{n},$$

12 said digital signature generating means being operative to transform said transmit
13 message word M to said signed ciphertext word C by performing a digital signature generating
14 process comprising the steps of,

15 defining a plurality of k sub-tasks in accordance with,

$$16 \quad C_1 \equiv M_1^{d_1} \pmod{p_1},$$

$$17 \quad C_2 \equiv M_2^{d_2} \pmod{p_2},$$

18 \vdots

$$19 \quad C_k \equiv M_k^{d_k} \pmod{p_k},$$

20 where,

$$21 \quad M_1 \equiv M \pmod{p_1},$$

$$22 \quad M_2 \equiv M \pmod{p_2},$$

23 \vdots

$$24 \quad M_k \equiv M \pmod{p_k},$$

$$25 \quad d_1 \equiv d \pmod{(p_1 - 1)},$$

$$26 \quad d_2 \equiv d \pmod{(p_2 - 1)}, \text{ and}$$

27 \vdots

$$28 \quad d_k \equiv d \pmod{(p_k - 1)},$$

29 wherein d is defined by,

$$30 \quad d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$$

31 e is a number relatively prime to $(p_1 - 1), (p_2 - 1), \dots, \text{ and } (p_k - 1),$

32 solving said sub-tasks to determine results C_1, C_2, \dots, C_k , and

33 combining said results of said sub-tasks to produce said signed ciphertext word C.
34

1 57. (Once Amended) A digital signature process comprising the steps of:

2 signing a plaintext message word M to create a signed ciphertext word C, wherein M
3 corresponds to a number representative of a message and wherein

4
$$0 \leq M \leq n-1$$

5 wherein n is a composite number formed by the product of $p_1 \cdot p_2 \cdot \dots \cdot p_k$, k is an integer
6 greater than 2[,] and p_1, p_2, \dots, p_k are distinct random prime numbers, C is a number
7 representative of a signed form of message word M, and wherein said encoding step
8 comprises transforming said message word M to said ciphertext word C whereby,

9
$$C \equiv M^d \pmod{n},$$

10 wherein d is defined by

11
$$d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}, \text{ and}$$

12 e is a number relatively prime to $(p_1 - 1), (p_2 - 1), \dots$, and $(p_k - 1)$; and

13 verifying said ciphertext word C to a receive message word M' by performing the steps

14 of,

15 defining a plurality of k sub-tasks in accordance with

16
$$M_1' \equiv C_1^{e_1} \pmod{p_1},$$

17
$$M_2' \equiv C_2^{e_2} \pmod{p_2},$$

18
$$\vdots$$

19
$$M_k' \equiv C_k^{e_k} \pmod{p_k},$$

20 wherein

21
$$C_1 \equiv C \pmod{p_1},$$

22
$$C_2 \equiv C \pmod{p_2},$$

23
$$\vdots$$

24
$$C_k \equiv C \pmod{p_k},$$

25
$$e_1 \equiv e \pmod{(p_1 - 1)},$$

26
$$e_2 \equiv e \pmod{(p_2 - 1)}, \text{ and}$$

27
$$\vdots$$

28
$$e_k \equiv e \pmod{(p_k - 1)},$$

30 solving said sub-tasks to determine results M_1', M_2', \dots, M_k' , and
31 combining said results of said sub-tasks to produce said receive message word
32 M' , whereby $M' = M$.

1 62. (Once Amended) A digital signature system comprising:

2 a communication medium;

3 [a] digital signature generating means coupled to said communication medium and
4 adapted for transforming a message word M to a signed ciphertext word C and for transmitting
5 said signed ciphertext word C on said medium, wherein M corresponds to a number
6 representative of a message, and

7 $0 \leq M \leq n-1$, wherein n is a composite number of the form

8 $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$,

9 wherein k is an integer greater than 2[,] and p_1, p_2, \dots, p_k are distinct random prime
10 numbers, and wherein said signed ciphertext word C corresponds to a number representative of a
11 signed form of said message word M and corresponds to

12 $C \equiv M^d \pmod{n}$,

13 wherein d is defined by

14 $d \equiv e^{-1} \pmod{(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_k - 1)}$, and

15 e is a number relatively prime to $(p_1 - 1), (p_2 - 1), \dots$, and $(p_k - 1)$; and

16 [a] digital signature verification means communicatively coupled with said
17 communication medium for receiving said signed ciphertext word C via said medium, and being
18 operative to verify said signed ciphertext word C by performing the steps of,

19 defining a plurality of k sub-tasks in accordance with

20 $M_1' \equiv C_1^{e_1} \pmod{p_1}$,

21 $M_2' \equiv C_2^{e_2} \pmod{p_2}$,

22 \vdots

23 $M_k' \equiv C_k^{e_k} \pmod{p_k}$,

24 wherein

25 $C_1 \equiv C \pmod{p_1}$,

26 $C_2 \equiv C \pmod{p_2},$
 27 \vdots
 28 $C_k \equiv C \pmod{p_k},$
 29
 30 $e_1 \equiv e \pmod{(p_1 - 1)},$
 31 $e_2 \equiv e \pmod{(p_2 - 1)},$
 32 \vdots
 33 $e_k \equiv e \pmod{(p_k - 1)},$
 34 solving said sub-tasks to determine results $M_1', M_2', \dots, M_k',$ and
 35 combining said results of said sub-tasks to produce said receive message word M'
 36 [whereby] wherein $M' = M.$

1 67. (New) A method as recited in claim 14 wherein said step of solving said sub-tasks
 2 includes processing each of said sub-tasks by an associated one of a plurality of exponentiator
 3 units operating substantially simultaneously.

1 68. (New) A method as recited in claim 14 wherein each of said distinct random prime
 2 number has the same number of bits.

1 69. (New) A method as recited in claim 15 wherein said step of solving said sub-tasks
 2 includes processing each of said sub-tasks by an associated one of a plurality of exponentiator
 3 units operating substantially simultaneously.

1 70. (New) A method as recited in claim 15 wherein each of said distinct random prime
 2 number has the same number of bits.

1 71. (New) A cryptographic communications system as recited in claim 16 wherein said step
 2 of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a
 3 plurality of exponentiator units operating substantially simultaneously.

1 72. (New) A cryptographic communications system as recited in claim 16 wherein each of
2 said distinct random prime number has the same number of bits.

1 73. (New) A method as recited in claim 17 wherein said step of solving said sub-tasks
2 includes processing each of said sub-tasks by an associated one of a plurality of exponentiator
3 units operating substantially simultaneously.

1 74. (New) A method as recited in claim 17 wherein each of said distinct random prime
2 number has the same number of bits.

1 75. (New) A cryptographic communications system as recited in claim 22 wherein said step
2 of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a
3 plurality of exponentiator units operating substantially simultaneously.

1 76. (New) A cryptographic communications system as recited in claim 22 wherein each of
2 said distinct random prime number has the same number of bits.

1 77. (New) A method as recited in claim 27 wherein said step of solving said sub-tasks
2 includes processing each of said sub-tasks by an associated one of a plurality of exponentiator
3 units operating substantially simultaneously.

1 78. (New) A method as recited in claim 27 wherein each of said distinct random prime
2 number has the same number of bits.

1 79. (New) A cryptographic communications system as recited in claim 32 wherein said step
2 of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a
3 plurality of exponentiator units operating substantially simultaneously.

1 80. (New) A cryptographic communications system as recited in claim 32 wherein each of
2 said distinct random prime number has the same number of bits.

1 81. (New) A method as recited in claim 37 wherein said step of solving said sub-tasks
2 includes processing each of said sub-tasks by an associated one of a plurality of exponentiator
3 units operating substantially simultaneously.

1 82. (New) A method as recited in claim 37 wherein each of said distinct random prime
2 number has the same number of bits.

1 83. (New) A cryptographic communications system as recited in claim 42 wherein said step
2 of solving said sub-tasks includes processing each of said sub-tasks by an associated one of a
3 plurality of exponentiator units operating substantially simultaneously.

1 84. (New) A cryptographic communications system as recited in claim 42 wherein each of
2 said distinct random prime number has the same number of bits.

1 85. (New) A method as recited in claim 47 wherein said step of solving said sub-tasks
2 includes processing each of said sub-tasks by an associated one of a plurality of exponentiator
3 units operating substantially simultaneously.

1 86. (New) A method as recited in claim 47 wherein each of said distinct random prime
2 number has the same number of bits.

1 87. (New) A digital signature generation system as recited in claim 52 wherein said step of
2 solving said sub-tasks includes processing each of said sub-tasks by an associated one of a
3 plurality of exponentiator units operating substantially simultaneously.

1 88. (New) A digital signature generation system as recited in claim 52 wherein each of said
2 distinct random prime number has the same number of bits.

1 89. (New) A digital signature process as recited in claim 57 wherein said step of solving said
2 sub-tasks includes processing each of said sub-tasks by an associated one of a plurality of
3 exponentiator units operating substantially simultaneously.